# CHAPTER 3

# COMBATTING TERRORISM

*"Kill one, frighten ten thousand."*
**Sun Tzu**

This chapter discusses terrorism and efforts by the commander to deter the threat of terrorism. It also presents measures and precautions that should be enforced across the operational continuum. The major focus must be on stopping a terrorist act before it happens. Vulnerability must be reduced by providing conditions unfavorable to the terrorist. The commander achieves success by not having a loss of life, equipment, or material through an act of terrorism. (See FM 100-37.)

## Section I. TERRORISM

To counter terrorism, the commander must understand terrorism. Also, he must know the countermeasures that reduce the chance of a successful terrorist attack against installations, units, and personnel.

### 3-1. DEFINITION

The DOD defines terrorism as "the unlawful use—or threat—of force or violence against people or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives." A terrorist's activities do not conform to rules or laws of warfare. His methods include hostage taking, hijacking, sabotage, assassination, arson, hoaxes, bombings, raids, seizures, use of NBC weapons, and so on. Victims are often noncombatants, symbolic persons and places, and political/military figures. Often the victims have no role in either causing or correcting a terrorist's grievance.

### 3-2. NATURE OF TERRORISM

The use of terrorism is not limited to the early stages of a conflict. It can and probably will occur in any level of conflict from peace through general war. Terrorist tactics are described as elusive, surprising, and brief violent actions.

### 3-3. COMMON STRATEGIES AND TACTICS

The common strategy of the terrorist is to commit acts of violence. These acts draw the attention of the people, the government, and the world to his cause. The media plays a crucial part in this strategy by giving terrorists international recognition. The danger is that this kind of attention tends to incite acts of violence by other terrorist groups.

a. The victim of the terrorist is seldom his target. The target, or focal point, more often includes the general public, government, or perhaps the business sector.

b. Some common tactics terrorists use include the following:

(1) *Bombing*. The tactic common to most terrorist groups is bombing. Of all terrorist incidents recorded during the 1980s, 67 percent resulted from the terrorist bomb. The bomb is a popular weapon, because it is cheap to produce, easy to make, has variable uses, and is difficult to detect and trace after the event. The increase in bombing

activity and the sophistication of devices used caused the NATO EOD Standardization Committee to classify all terrorist bombs as improvised explosive devices (IEDs). The term IED is now used by many law enforcement agencies as well as military forces. Some IED subclassifications include:

(a) Delivery means. Methods of getting the bomb to the target.

- Vehicle bombs—booby-trapped vehicles, attached devices, and car bombs (cars filled with explosives).
- Laid charges—bombs placed by hand.
- Projected bombs—bombs thrown by hand or projected by a mortar device.
- Postal bombs.
- Bicycle bombs.

(b) Activation means. Three ways to activate an IED.

- Command activation—by radio, electric leads, pull wire/mechanical strikers.
- Action by the subject/target—trip wire, pressure device, light sensitive device, electric.
- Time delay—clock, burning fuse, chemical delay, atmospheric pressure.

(c) Usage. Two broad classifications.

- Tactical improvised explosive devices (IED)—normally regarded as being those used against an individual. These include nail bombs, claymore devices, and covert bombs. In fact, any IED can be classified as a tactical IED.
- Strategic IEDs—considered to be those used indiscriminately to gain world attention—for example, in crowded shopping centers, on aircraft, and so on. They are those bombs designed to strike at society, the government, and the present system.

(d) Hoaxes. Whatever the type of IED, the terrorist often uses it to gain recognition and to show he is serious. Once he has established himself as a bomber, he can continue to disrupt, though not destroy, by using well-made and well-placed hoax bombs. The use of hoaxes with live IEDs can keep security forces occupied and disrupt counterterrorist operations.

(2) *Arson*. Although not a popular tactic among terrorists, arson can destroy and disrupt such targets as public utilities, political headquarters, and, more commonly, economic/industrial targets (shops, factories, hotels). The most popular method of starting fires is with time-delay incendiary devices, often carried in a cigarette packet or cassette tape container. These devices are easy to conceal and difficult to detect. As with bombing, incendiary devices are cheap and easy to make.

(3) *Hijacking*. Hijacking and skyjacking were common during the 1960s, 1970s, and early 1980s. Hijacking of vehicles carrying staple foods was a favored tactic of the Supemaros and suited their style of armed propaganda. The hijacking would be followed quickly by the free distribution of the vehicle's cargo to the poor and needy along with terrorist propaganda that advertised the terrorists' cause. In any continuing terrorist activity, such as in Spain or Northern Ireland, the hijacking of a vehicle will likely be associated with a future atrocity. For example, a hijacked gasoline truck may appear later as a 50,000-pound benzine bomb wired with explosives. Also, hijacked "legitimate" vehicles give the terrorist an easy means to gain entry to a closed military post.

(4) *Ambush*. Well-planned ambushes seldom fail. Ambushes usually include the use of diversions and early-warning teams. Properly rehearsed, they are executed with precision. The terrorist has time on his side and spends weeks or months preparing for an operation and waiting for the right opportunity. The terrorist can chose his own time and place of operation and, if his intended victim habitually uses the same route, the terrorist can conduct countless rehearsals before execution.

(5) *Kidnapping*. Not all ambushes are designed to kill the principal. Kidnapping for ransom accounted for 7.9 percent of terrorist incidents in the last decade and must still be viewed as a serious option for terrorist groups. The kidnapper confines his victim in a secret hideaway and makes material demands (money, weapons, exchange of personnel, and so on). A failed kidnapping may result in hostage taking.

(6) *Hostage taking*. The difference between hostage taking and kidnapping is minimal. The

hostage taker normally confronts authorities and openly holds his victims for ransom. The hostage taker demands more than just material things—political concessions are often demanded in exchange for the lives of the hostages. Hostage taking is a new and popular terrorist tactic. By its nature, hostage taking attracts the media; the fact that live hostages are involved increases the drama of the event. The hostage is a tangible asset with which to bargain. Therefore, terrorists can apply pressure to force concessions that otherwise might not be made. Through kidnapping and hostage taking, terrorists can acquire large gains at minimal cost, although risks are involved.

(7) *Assassination.* Assassination is perhaps the oldest terrorist tactic and is still used today. Targets are often predictable, and terrorist groups claim them after the event. Targets include government officials, corporate executives, police, military personnel, and security officials.

(8) *Other tactics.* Whatever tactics terrorists use, they are simple to apply, dynamic in effect, hit-and-run by nature, and designed to strike their objective rather than the victim. Terrorists will always do a thorough reconnaissance and a detailed plan. Time is not a factor. Commanders must be aware of the tactics of potential terrorists in their AOR. Other possible tactics include the use of chemicals, harassment, raids, sabotage, seizures, and maimings.

## 3-4. INTERNATIONAL NETWORK

Terrorist groups today do not operate alone and ignorant of one another. An international network exists that provides great benefits for those who have paid their "membership fee." It is not suggested that some international headquarters plans terrorist acts across the globe. However, it is proven that a type of international terrorists' support network does exist. The benefits gained from such a network seem endless: arms, ammunition, money, intelligence, explosives, safe houses. Most important is the experience and assistance given in training and support facilities. Along with the resultant trained manpower, the network grows.

## 3-5. CATEGORIES OF TERRORIST GROUPS

A terrorist group's choice of targets and tactics is also a function of the group's government affiliation. They are categorized by government affiliation. This helps security planners foresee terrorist targets, and his sophisticated intelligence and weaponry. Terrorist groups are divided into three categories:

a. **Nonstate supported**—a terrorist group that operates autonomously, receiving no support from any government.

b. **State supported**—a terrorist group that operates alone but receives support from one or more governments.

c. **State directed**—a terrorist group that operates as an agent of a government, receiving substantial intelligence, logistic, and operational support.

## 3-6. TERRORIST OBJECTIVES

The immediate objective of any terrorist attack normally complies with one or more categories. The goals may be either immediate or long range. Terrorists demonstrate group power, demand revenge, obtain logistic support, and cause a government to overreact. They are recognized by coercion, intimidation, and provocation. At the same time, terrorists gain support for themselves or an insurgency.

a. **Immediate Goals.**

(1) Obtain worldwide, national, or local recognition for their cause.

(2) Force government reaction, overreaction, and repression leading to immediate public dissension.

(3) Harass, weaken, or embarrass government, military, or other security forces.

(4) Obtain money or equipment.

(5) Show a government's inability to protect its citizens.

(6) Disrupt or destroy primary means of mobility or communications.

(7) Demonstrate power or threat credibility.

(8) Prevent or delay decisions or legislation.

(9) Cause strikes or work slowdowns.

(10) Discourage impending foreign investments or foreign government assistance programs.

(11) Free prisoners.

(12) Seek vengeance.

b. **Long-Range Goals.**

(1) Cause dramatic changes in government such as revolution, civil war, or war between nations.

(2) Disrupt and discredit an established infrastructure in support of an insurgency.

(3) Influence local, national, or international policy decision making.

(4) Gain political recognition as the legal body representing an ethnic or national group.

### 3-7. TERRORIST TARGETS

Anyone or anything can be a target or victim of a terrorist act. However, to the terrorist, the military represents a source of arms and material as well as a political or national body. This places the military at great risk. The list below contains some possible military targets of terrorists; it provides some areas of concern. Targets may change as security is increased.

- Sensitive night vision and communication items.
- Arms.
- Ammunition.
- Command and control facilities.
- Explosives.
- Military officer training facilities.
- Areas catering to personal needs (mess halls, barracks, post exchange, commissary, gyms, religious activities, bars, community centers).
- Hydroelectric plants, dams, gas pipelines, nuclear facility sites.
- Communication lines/facilities, computer facilities.
- Chemical storage sites.
- Equipment warehouses.
- Transportation centers, parking lots, airports, railheads, bus depots, rail lines, shipyards.
- Members of military force and their dependents.
- Key leaders of the military.
- Post offices and mail trucks.

## Section II.
## ANTITERRORISM AND COUNTERTERROISM

Combatting terrorism consists of two major categories. The commander must develop a plan that includes the aspects of antiterrorism and counterterrorism. The plan should reduce the vulnerability of installations, units, and personnel during peacetime, predeployment, deployment, and redeployment. It should also include measures for preventing, deterring, and responding to terrorism.

### 3-8. ANTITERRORISM

Installations, units, and individuals employ antiterrorism measures to reduce the chance of falling victim to a terrorist act. These measures are considered both active and passive, designed to prevent a terrorist incident. They must involve each member of the military community—military, civilian, and family members. The cornerstone for this program includes collecting and disseminating timely threat information, conducting information awareness programs, and implementing sound defensive measures. Three types of security measures to consider are physical security, OPSEC, and personal security.

a. **Physical Security.** Physical security measures protect information, material, and persons, as well as prevent criminal acts. Although terrorist activities are criminal acts, there are some differences that must be considered when providing physical security against terrorists. Terrorists are likely to be more organized, better trained and educated, and more highly motivated than other criminals. They are heavily armed and sophisticated in their ability to defeat physical security measures. To provide physical security against terrorists, leaders must consider the terrorist whose goal may include his own self-destruction. This is different from security against other criminals or a conventional enemy. Several actions can help determine what physical security measures are needed.

(1) Review crime-prevention surveys/inspections. These surveys consider the entire

installation as well as the effect on the surrounding civilian locale.

(2) Provide photos of known terrorists to key personnel. These photos can be obtained through local civilian and military authorities. The photos can also be prominently displayed in common areas so that all personnel have access to them.

(3) Review physical security surveys/inspections. This survey recommends action as a result of on-site inspection of barriers, guard forces, communications, transportation, contingency support, protective lighting, intrusion lighting, intrusion detection system, and other physical security measures. These actions protect installations from loss, theft, destruction, sabotage, or compromise.

(4) Review status of work orders; establish the priority of work based on threat assessment.

(5) Determine if the installation is closed or open. It is closed if ground and water access is limited by a perimeter fence, controlled entry points, or other physical barriers. If not, the commander must compensate by designating restricted areas, providing entry control, and maintaining contingency plans to secure or close all or part of the installation.

(6) Consider physical security aspects.

- Protective obstacles and barriers.
- Electro-optical and night vision equipment.
- Bomb threats.
- Closed-circuit television.
- Communications.
- Entry control.
- Intrusion detection systems.
- Lighting.
- Lock and key control.
- Package and mail control.
- Personnel reliability.
- Location of restricted areas.
- Inspection of water and food.
- Inspection of key personnel vehicles.

The physical security plan must be balanced in its orientation, with equal emphasis on preventing criminal acts as well as terrorist acts. The commander must update his plan continuously based on threat assessment.

b. **Operational Security.** Protecting information is the cornerstone of the OPSEC program. The OPSEC program coordinates all actions needed to prevent an enemy or terrorist from learning about plans and operations. Techniques of deception, physical security, SIGSEC, and information security are interrelated and occur at the same time. All planning must include measures to keep the potential terrorist from obtaining information that could aid in a terrorist incident. Four areas of information that terrorists can exploit are as follows:

(1) *Human intelligence.* HUMINT involves using people to gather information about military abilities and intentions to include installation day-to-day activities. HUMINT sources can include seemingly unimportant bar or restaurant conversations concerning operations, or the release of phone numbers and addresses of key personnel. This threat can be countered by adhering to physical security and information security practices, and by using countersurveillance and counterintelligence activities.

(2) *Signal intelligence.* SIGINT concerns all forms of communications and signal emission equipment. Terrorists may not be able to compromise sophisticated equipment, but they can affect routine day-to-day communications activities. For example, police or fire department frequencies are not changed when radios are stolen, or telephones in sensitive areas are not checked for bugging devices. This threat is countered by establishing communications security and information security.

(3) *Photo intelligence.* Terrorists use PHOTOINT to gain information through coverage from aircraft, high terrain features, automobiles, and so on. PHOTOINT can be countered through counterintelligence and countersurveillance programs.

(4) *Operational patterns.* Operational patterns of military organizations provide information to a terrorist. To counter this threat, leaders must eliminate patterns when possible. Otherwise, they should use deception measures to mask the established pattern.

c. **Personal Security.** No person is immune to the threat of terrorism. Representatives of the US Government are possible targets of terrorist activities. Terrorists may preselect offices, manufacturing plants, or other installation assets as targets for bombing, sabotage, demonstrations, abductions, and murders. Who occupies these buildings may be of little concern to the terrorists. Measures that may be useful in deterring such acts are as follows:

(1) Control access to sensitive areas and command offices, both day and night.

(a) Prevent direct access to sensitive areas most likely to be targets of terrorism. Do not locate command offices on the ground floor.

(b) Equip entrances to sensitive areas and command offices with an alarm.

(c) Have an access roster; escort visitors.

(d) Ensure direct-security force personnel check command areas in their after-hours tour.

(e) Lock all restrooms on floors where command offices are located (as well as others in a multistory office building) to deter public access.

(f) Lock doors to janitorial and other maintenance closets at all times.

(g) Lock doors to telephone and electrical equipment rooms. Give access to maintenance and telephone personnel only when they have such need.

(2) Select an interior safe room for use if terrorists attack; do not identify it as a safe room.

(3) Maintain emergency supplies such as first-aid equipment, bomb blankets, candles, rations, water, lanterns, and so on. Inform key personnel as to where supplies are kept, and the location of emergency exits and escape routes.

(4) Restrict the personal history data on key personnel since this information could be used by terrorists to select victims or to identify their homes and families.

(5) Recommend key personnel parking areas not be identified by name but rather by number.

(6) Limit information on travel agendas and plans of command or key personnel to only need-to-know personnel.

(7) Increase the effect of command and key personnel protective measures by encouraging them—

(a) To maintain a low profile.

(b) To be taught to recognize the signs of surveillance by strangers.

(c) To use simple, effective, verbal code signals to alert family or organizational members to a physical threat.

(d) To vary routes to and from work.

(e) To attend defensive and evasive driving school.

(f) To inspect vehicles before moving.

(g) To use protective vests.

(h) To avoid likely terrorist targeted areas.

(i) To drive with windows closed and doors locked.

(j) To know key phrases in the native language.

(k) To carefully screen all domestic help.

(l) To know terrorist techniques and methods of operation.

(m) To perform roadmap reconnaissance to avoid suspected terrorist concentrations when traveling to new destinations (restaurants, hotels, shopping, and so on).

## 3-9. TERRORIST THREAT CONDITIONS

The following terrorist threat conditions describe progressive levels of terrorist threat to US military facilities and personnel. As Joint Chiefs of Staff-approved terminology, these terms, definitions, and security measures implement a standardized terrorist alert system throughout the DOD. MACOMs and subordinate commands are not authorized to change the basic system; however, supplements to the system may be published. The selection of appropriate responses to terrorist threats remains the responsibility of the commander having jurisdiction or control over threatened facilities or personnel.

a. **Threat Condition Alpha (Low).**

(1) *Definition.* A general threat of possible terrorist activity against installations and personnel, of unpredictable nature and extent, when circumstances do not justify full implementation of measures contained in a higher threat condition. Selected measures from higher threat conditions may be implemented as needed.

(2) *Measures To Be Taken.*

(a) At regular intervals, remind all personnel, including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; to be alert for unidentified vehicles on or near US installations; and to be alert for abandoned parcels or suitcases, or for any unusual activity.

(b) Keep the duty officer or other appointed personnel available to evacuate buildings and areas, and to seal off areas where an explosion or attack has occurred. Keep key personnel on call to implement security plans.

(c) Secure buildings, rooms, and storage areas not in regular use.

(d) Increase security spot checks of vehicles and persons entering installations and nonclassified areas under the jurisdiction of the US command and agency.

(e) Limit access points for vehicles and personnel.

(f) As a deterrent, apply one of the following measures from threat condition Bravo individually and randomly:

- Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
- At the beginning and the end of each workday, and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages.
- Check all deliveries to installation activities and advise dependents to check all home deliveries.
- As far as resources allow, increase surveillance of domestic accommodations (schools, messes, clubs, and other soft targets) to improve deterrence and defense, and to build confidence among the staff and dependents.

(g) Review all plans, orders, personnel details, and logistic requirements related to the introduction of the higher threat condition.

(h) Review and implement security measures for high-risk personnel.

**b. Threat Condition Bravo (Medium).**

(1) *Definition.* An increased and more predictable threat of terrorist activity even though no particular threat has been identified.

(2) *Measures to be Taken.*

(a) Remind all personnel to be cautious and inquisitive about suspicious persons, vehicles, and activities. Warn personnel of any form of attack to be used by terrorists.

(b) Keep all personnel on call who are involved in implementing antiterrorist contingency plans.

(c) Check plans for implementing measures contained in the next threat condition.

(d) Where possible, move cars and other objects at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the use of centralized parking.

(e) Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

(f) Make regular and frequent inspections of the interior and exterior of buildings for suspicious packages.

(g) Thoroughly examine all mail for letter or parcel bombs.

(h) Check all deliveries to installation activities and advise dependents to check all home deliveries.

(i) As far as resources allow, increase surveillance of domestic accommodations (schools, messes, clubs, and other soft targets) to improve deterrence and defense, and to build confidence among the staff and dependents.

(j) Keep the staff and dependents informed of the general situation to stop rumors and prevent unnecessary alarm.

(k) At an early stage, inform members of local security committees of any action being taken and why.

(l) Upon entry of visitors to the unit, physically inspect them and a percentage of their suitcases, parcels, and other containers.

(m) Wherever possible, operate random patrols to check vehicles, people, and buildings.

(n) Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a car.

(o) Implement additional security measures for high-risk personnel.

(p) Brief personnel who may augment the guard force on directives and regulations concerning the use of deadly force.

(q) Conduct a random search of vehicles entering the installation.

**c. Threat Condition Charlie (High).**

(1) *Definition.* A terrorist incident has occurred or intelligence has been received indicating that some form of terrorist action is imminent.

(2) *Measures to be Taken.*

(a) Continue all threat condition Bravo actions or introduce those not already implemented.

(b) Keep all personnel on duty who are responsible for implementing antiterrorist plans.

(c) Limit access points to absolute minimum.

(d) Strictly enforce control of entry and search all vehicles.

(•) Enforce centralized parking of vehicles away from sensitive buildings.

(f) Issue weapons to guards. (Local orders should include specific instructions on issue of ammunition.)

(g) Increase patrolling of the installation.

(h) Protect all designated vulnerable points and give special attention to vulnerable points outside military establishments.

(i) Erect barriers and obstacles to control traffic flow.

d. **Threat Condition Delta (Imminent).**

(1) *Definition.* Terrorist attack has occurred in the immediate area or intelligence has been received that terrorist action against a specific location is likely. Normally, this threat condition is declared as a localized warning.

(2) *Measures To Be Taken.*

(a) Continue or introduce measures listed for threat conditions Bravo and Charlie.

(b) Augment guards, as needed.

(c) Identify all vehicles already on the installation within operational or mission support areas.

(d) Search all vehicles entering the complex or installation as well as vehicle contents.

(e) Control all access and implement positive identification of all personnel.

(f) Search all suitcases, briefcases, and packages brought into the complex or on the installation.

(g) Enforce measures to control access to all areas under the jurisdiction of the US command or agency concerned.

(h) Check often the exterior of buildings and of parking areas.

(i) Minimize all administrative journeys and visits.

(j) Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attack.

e. **Threat Assessment Guidelines.** The following general guidelines provide for uniform implementation of security alert conditions. Assessment factors are defined as—

(1) *Existence.* Applies when a terrorist group is present in an area of concern. The group need not have posed a threat to US or DOD interests in the past.

(2) *Capability.* Applies when a terrorist group has the ability to implement an operation against US interests in areas of concern. This includes resources such as intelligence, mobility, personnel, and equipment (explosives, arms, and ammunition).

(3) *History.* Applies when a group's history of terrorist acts and behavior reflects an anti-US stand or includes previous attacks against US interests.

(4) *Trends.* Applies if the group has, over the past year, displayed terrorist activity that appears to be continuing or increasing. Activity need not have been violent; terrorist attacks against US or DOD interests may be merely threatening statements.

(5) *Targeting.* Applies if there are known plans or confirmed intentions of a terrorist group to target US or DOD interests. Targeting can be either specific or nonspecific. If targeting is not against US or DOD interests, this factor should not be considered.

A combination of positive answers to any or all of the above assessment factors will produce a threat level of either low, medium, high, or imminent. These guidelines apply only to the assessment of terrorist threat against US or DOD interests.

f. **Threat Condition Reporting Procedures.** Department of the Army requires MACOMs that own installations to implement a reporting system within their respective commands. This system will provide DA and senior Army leaders current information on the antiterrorist posture so that resources are dedicated where they are most needed. (See applicable regulations for reporting procedures.)

## 3-10. COUNTERTERRORISM

Counterterrorism includes the full range of offensive measures to prevent, deter, and respond to terrorism. This is the final phase in combatting terrorism. It is reactive and validates the extensive preparation, planning, and response measures established in terrorism counteraction plans. The type of forces and command and control relations used in counterterrorism operations depend on the location, type of incident, and degree of force required. Force selection criteria are governed by legal and political constraints. Some military operations executed by US forces in response to terrorist acts may be carried out by conventional forces, However, usually these forces provide support to a specially organized, equipped, and trained counterterrorism unit. In executing counterterrorism actions, leaders should ensure organizational planning addresses the following tasks:

a. **Intelligence.** A well-planned, organized, all-source intelligence program is vital in order to identify the threat and to provide timely threat intelligence. (See Chapter 6.) This includes evaluating terrorist abilities, tactics, and strategy.

b. **Hostage Negotiations.** Due to jurisdictional considerations, hostage negotiations are normally the responsibility of another US government agency or the host nation.

c. **Hostage Rescue.** Specially organized, trained, and equipped personnel and units are maintained to rescue and protect hostages.

d. **Assault of Terrorist Positions.** An objective of national policy is to deter the terrorist through the threat of retaliation. When this becomes necessary, US military personnel normally conduct the operation. This mission could be assigned to either special operations forces, conventional forces, or both. If SOFs are used, the US military commander must still plan to establish an inner security perimeter of MP units. He also establishes an outer security perimeter of soldiers and a special reaction element to respond to other isolated incidents within the AOR.

## Section III.
## COMBATTING TERRORISM IN LIC

Commanders must take action to counter terrorists. During peacetime, they must develop and employ antiterrorist plans. The measures to deter, prevent, and respond to threat are based on the terrorist threat conditions. The plan must correspond to and be included in the security plan. This includes physical security, OPSEC, and personal security. As the unit deploys for COIN operations, PKOs, or PCOs, the chances of a terrorist act increases. Based on the threat, commanders must guard unit personnel and equipment.

### 3-11. DEPLOYMENT IN CONTINGENCIES

A commander with a deployment mission must reduce the vulnerability of his unit to terrorist attack. These precautions must be included during predeployment, deployment, and redeployment.

a. **Predeployment.** The commander must develop his unit's security to complicate the terrorist's decision making. As he plans his concept of the operation, he assesses the threat. From this, the operational plans, equipment, and special skills can be chosen that increase risk to the terrorists.

(1) The concept should—

(a) Include security against terrorism in all orders, plans, and training.

(b) Include security in the commander's guidance.

(c) Deter or create risk for the terrorist through security programs.

(2) The planning process must include—

(a) Mission analysis.

- How can the mission be affected by a terrorist attack?
- What are the security aspects of both specified and implied tasks?
- Continue to review unit weaknesses throughout predeployment, deployment, and redeployment.

(b) Threat assessment.

- Identify terrorist groups operating in the deployment area.

- Develop a list of PIR: methods of operation, attack methodology, and preattack indication.
- Identify sources of information on terrorist groups; know how to access them quickly and routinely.
- Routinely include threat assessment in intelligence estimates.

(c) Combat service support considerations.

- Procurement of special security equipment (Table 3-1).
- Protection of storage and distribution areas.
- Maintenance of special equipment.
- Security of maintenance unit if separate from main body.
- Security during movement (based on threat).
- Security in staging areas.
- Liaison with security agencies that support the move or with controlling areas that move (host country).

(d) Combat support considerations.

Engineering priority of work based on the mission and terrorist threat.

Special engineer equipment for conducting countermine and EOD; protective obstacle emplacement; constructing roadblocks; critical site, asset, and troop protection.

Special engineer equipment.

Engineer training to maneuver units on visual detection/recognition of mines/booby traps.

MP check/inspect/improve unit physical security.

MP liaison with local police/security personnel.

MP assist in security planning and training.

Host nation security forces assisted by MP screen civilian and host nation employees.

No hiring of civilian employees, if possible.

If employed, special security procedures for screening and monitoring civilians.

| GENERAL | ROADBLOCKS | SEARCHES | SPECIALISTS | ENGINEERS |
|---|---|---|---|---|
| Pyrotechnic pistols<br>Riot guns<br>Tear gas launchers<br>Hand-held flashlights<br>Antiriot helmets<br>Shields 3ft 6in<br>Shields 6ft<br>Police batons<br>Handcuffs<br>Body armor<br>Marshalling wands<br>Telescopes and tripods<br>Binoculars<br>Infrared devices<br>Loud speakers<br>Fire extinguisher<br>Cameras with flash attachments and tripods<br>Telesopic sights<br>Photographic filter<br>Polaroid cameras<br>Whistles<br>Hand-held radios (for use in urban areas) | Portable lamps/lights<br>Marker lights<br>Traffic cones<br>Traffic signs<br>Visor sleeves<br>Car punture chains<br>Directional arrow<br>Lightweight barriers<br>Mirrors | Ladders<br>Flashlights<br>Picks,shovels<br>Wrecking bars<br>Hand tools, florescent (hammers, pliers, screwdrivers)<br>Rope<br>Magnets<br>Telescopic mirror<br>Axe<br>Mine markers<br>Hemets<br>White tape<br>Mine detectors<br>Eye shields<br>Measuring tape<br>Metal cutting tools<br>Chisels<br>Knives<br>Saws<br>Mine probes<br>Safety harness | Explosive detectors<br>Remote light unit<br>Remote-controlled EOD device<br>Endoscope<br>Engineer heavy equipment<br>Concrete mixers<br>Mobile lighting<br>Portable compressor<br>Hydraulic platform<br>Engineer tractors<br>Platform hoist<br>Equipment in static defense column<br>X-ray equipment<br>Metal detectors | Portable sensors<br>Portable alarms<br>Portable lighting system<br>Barriers (drop arm and swing arm)<br>Roadblock equipment for exit/entry control<br>Closed-circuit TV<br>Shot direction indicator<br>Barbed wire<br>Wire netting<br>Corrugated iron<br>Fence materials<br>Steel girders<br>Scaffolding |

Table 3-1. Specialized equipment.

- In many countries, a fee for information is expected. Coordinate with the State Department for a means to pay for information.

(e) Operational considerations.

- Unit plans. Include security in each plan, SOP, OPORD, and movement order.
- Security plans. Prepare, review, and update unit security plans (physical security, crime prevention, and so on), and individual security plans (guard orders).
- Security programs. Develop specific security programs such as threat awareness and OPSEC.
- Special teams. Due to the terrorist threat, consider a different task organization (search teams, special reaction teams, protective service teams).
- Special skills. To counter the terrorist threat, add special skills to units (interrogators, linguists, FAOs, EOD personnel, public affairs, SOF liaison, CA officer). Some may need to go with advanced parties.
- Command and support relationships. These may differ from the routine (State Department, host nation, country team, SOF teams). Resolve command and support relationships between the advance party of the JTF and the brigade and other agencies before deployment.

(f) Specialized skills training. Institutional training for specialized skills (instructor qualification, evasive driving, special reaction teams, threat awareness, search techniques, hostage negotiation, roadblocks, sentry duties, joint police action with host country).

(g) Transit to deployment area.

- Consider overall security of the unit throughout the entire movement: emergency action procedures, alternative routes or diversions, and organic security teams with each movement element.
- Implement en route planning and training.
- Immediately update intelligence/threat assessment before arrival.

b. **Deployment.** Deployment is the second stage of the mission. As units move and establish operation bases, commanders must not create lucrative targets.

(1) *Advanced party considerations.*

(a) Composition. More personnel are needed for security and liaison with host nation security agencies, because a means for added intelligence on terrorism is required.

(b) Deployment. The primary security consideration for the advanced party is whether it should be standard or low profile (uniform or plain clothes, military or civilian transport).

(c) Validation. The advanced party must validate the mission and PIR. Required tasks include determining if the terrorist threat assessment tracks with actual threat and if the threat from in country affects the accomplishment of the mission; and, discovering the mission, if it is the same as the commander's.

(d) Rules of engagement. The advanced party must confirm planned rules of engagement. It must determine if they are the same as those during the predeployment phase. Problems must be resolved before the main body arrives.

(2) *OPSEC measures in deployment.*

(a) Avoid making known the time and place of arrival; otherwise, increase security.

(b) Avoid setting patterns of behavior/operation.

(c) Set up secure communications with main body and advanced party.

(3) *Pass policy.* On extended operations, the morale of soldiers must be considered. A pass policy may be established in the mission area. However, soldiers must keep a low profile. Commanders should do the following:

(a) Provide troop information briefings on the threat.

(b) Establish pass policies using the buddy system.

(c) Establish off-limits areas.

(4) *Force protection.* In setting up operating bases and in day-to-day operations, commanders must consider the security of his forces. This is a major concern when the rules of engagement are restrictive. Some considerations are as follows:

(a) Coordinate with security forces that protect forces (MP, host nation forces, directing staff).

(b) Avoid providing lucrative targets (troop concentrations, motor pools, large static logistic installations).

(c) Transit within deployment area.

(d) Continue threat assessment along routes for each movement.

(e) Include security in all movement orders.

(f) Provide security at departure and arrival points.

(g) Employ security forces during transit.

(h) Establish liaison and coordinate with all security agencies along route.

(5) *Security enhancement.* Commanders should use TOE and specialized equipment to provide security based on threat assessment.

(a) Assign the provost marshal or a military police officer the responsibility for physical security.

(b) Ensure all personnel know the governing regulations (guard orders, rules of engagement, local restrictions).

(c) Stay aware of training and the troop information program.

(d) Include force/base protection when arranging unit positions (good defense/barrier plan, dispersion of high-value targets away from access roads, perimeter fences).

(e) Maintain a low profile (restrict passes).

(f) Restrict access of unassigned personnel to the unit's location. Restrict the number of vehicles within perimeters and keep parking away from buildings. Perform stringent identification checks.

(h) Constantly portray an image of professionalism and readiness.

(i) Continue to reassess the environment.

c. **Redeployment.** During the redeployment phase, preparing for a terrorist attack is as vital as during the other phases. In fact, units tend to relax after an operation. Redeployment depends on the mission, the publicity, and the international reaction. It may be the most vulnerable phase for a terrorist attack.

(1) The advance party must keep a security alert and awareness posture until all of the unit has returned. The advance party should develop PIR for return to home station.

(2) Stay-behind personnel are most open to terrorist attack since the armed presence is less. They must keep a security posture that reflects the chance of a greater threat. Actions include maintaining liaison with security forces, adding to security measures, and keeping tight controls on personnel.

(3) The following should be considered for reverse deployment:

(a) The security of the port of entry and lines of communications for the return trip.

(b) If the mission has changed the situation at home. An unpopular political decision may expose the unit to a threat upon its return to the US.

(c) To adopt the security measures used during transit to, and movement within, the deployment area. Coordinate reaction ability with security agencies along the route.

(4) A coordinated PAO policy should be developed to incorporate the following:

(a) Control of information released to the media ensures accuracy and completeness.

(b) Troops should be briefed as to release of information to outside agencies. Only public affairs personnel have release authority.

(5) Debriefing should be conducted. The stress increase in soldiers during intense deployment operations must be allowed to subside. This helps to adjust back into a peacetime environment. These debriefings include:

(a) Briefing soldiers to change their orientation from LIC duty back to peacetime.

(b) Updating soldiers regarding new policies, incidents, or threats that developed since the deployment operation.

(c) Inspecting soldiers for maps, souvenirs, ordnance, and weapons.

(6) A thorough after-action report should be prepared. It provides two vital services for units that conduct future operations. It provides future commanders a benefit from lessons learned. Also, it serves as a resource for validating terrorism counteraction procedures for future operations.

## 3-12. PRIORITY INTELLIGENCE REQUIREMENTS AND LOCAL TERRORISM INDICATORS

Combatting terrorism, more than any other form of warfare, requires knowledge of the enemy's goals and abilities. Intelligence officers, supporting a deploying unit, must always consider the terrorist's concerns when developing EEIs and a list of local terrorism indicators.

a. **Priority Intelligence Requirements.** The following terrorist concerns can assist the intelligence officer in developing PIR:

- Organization, size, and composition of group.
- Motivation, long-range goals, and short-range goals.
- Religious, political, ethnic affiliation, or a combination of these.
- International and national support (moral, physical, financial).
- Recruiting methods, locations, and targets (students).
- Identities of group leaders, opportunist, and idealists.
- Group intelligence abilities.
- Sources of supply/support.
- Important dates (religious holidays, martyrdom anniversaries).
- Planning competence.
- Degree of discipline.
- Preferred tactics and operations.
- Willingness to kill.
- Willingness for self-sacrifice (professed or demonstrated).
- Group skills (sniping, demolitions, masquerade, forged documents, industrial sabotage, airplane/boat operations, tunneling, underwater electronic surveillance, poisons/contaminants).
- Equipment and weapons on hand and required.
- Transportation on hand and required.
- Medical support available.
- Freedom of access to media and skill in using it.

b. **Local Terrorism Indicators.** Some conditions that may indicate politically motivated violence in certain locations are as follows:

(1) Dissent for political, social, or ethnic reasons. Charges brought against local government.

(2) Formation of radical groups, branches of national subversive groups, or secret societies.

(3) Antigovernment, anti-US agitation; identification of government or US as the root of the problems.

(4) New spokesmen for the people's causes emerging; out-of-town organizers arriving.

(5) Meetings, rallies, and demonstrations beng organized; grievances taking political overtones; inflammatory speeches and charges made; provocation of authorities to intervene, or overreact; police or military brutality charged.

(6) Appearance of antiestablishment posters, leaflets, underground press; taking people's concern into political arena; politicization of social causes.

(7) Use of known personalities as draws for rallies, especially those that have been identified with radical causes.

(8) Demonstrations, civil disobedience, or protest marches with causes overshadowed by political rhetorics.

(9) Increased recruiting, by known front groups and radical organizations; support sought among workers.

(10) Increased activism in political spheres at colleges and universities.

(11) Speeches and communications stating violence as the only means of solution.

(12) Identification of foreign influence or aid.

(13) Threats against public works, utilities, or transportation; threats of violence against prominent personalities.

(14) Agitation in refugee, minority, or foreign communities; polarization; arming segments of society.

(15) Reports of stolen firearms and explosives; raids on armories, and sporting goods stores.

(16) Violence against property, looting, destruction, and arson; mainly during demonstrations, marches, or mob actions.

(17) Violence against persons, murders, attempted murders, beatings, threats, abductions, or public targeting of people.

(18) Increased purchases of high-performance weapons; appearance of automatic weapons, mainly of foreign manufacture.

(19) Discovery of weapons, ammunition caches, and explosives; indication of terrorist training; increased terrorist surveillance.

(20) Open attacks on police, military, and other authorities.

(21) Reports of stolen identification cards, membership cards, and so on.

### 3-13. OPERATIONS SECURITY MEASURES

Commanders can implement certain measures to avoid stereotyping and to deny intelligence information to the enemy.

a. Commanders should adhere to the following OPSEC measures:

(1) Use EEFI to guide the OPSEC program. Develop EEFI—those items/activities of planning that terrorists can use.

(2) Present random action in unit operating procedures (change patrol schedules, routes, check points, sentry, or guard positions.

(3) Avoid any set pattern for commanders, meetings, meal schedules, resupply activity, religious services, or sentry or guard reliefs.

(4) Employ protective obstacles (perimeter and internal).

(5) Check identification of all personnel entering and leaving the perimeter or installation.

(6) Employ added security to restricted areas (communications posts, communication centers, motor parks, high-density troop areas).

(7) Control distribution of itineraries of VIPs/high-risk personnel.

(8) Establish dismount points and parking areas away from buildings. If possible, these should not be seen from outside the base.

b. The following are examples of intelligence indicators that might assist a terrorist in gathering intelligence on a unit. This is a sample listing and should not be construed as all inclusive.

(1) *Operation Indicators.*

(a) Troops restricted to the post before a move or operation.

(b) Increased patrolling/air reconnaissance.

(c) No patrolling at all.

(d) Increased movement between locations caused by task organizations before an operation.

(e) Special requisitions to increase rations, transport, and ammunitions.

(2) *HUMINT Indicators.*

(a) Newspaper or other media coverage.

(b) Farewells and last-minute visits by VIPs or senior officers.

(c) Church services the night before an operation.

(d) Bulletin notices stating that enforced rest is required; dispensary hours are changed.

(e) Public signs announcing changes in procedures (restricting civilian travel/access).

(f) Photography developed by local contractors showing in-camp scenes and preparations.

(3) *Communication Indicators.*

(a) Change in call signs and frequencies before an operation.

(b) Movement of auxiliary communication equipment (new aerials) to a new area.